Math 116: Problem Set 7

Owen Jones

March 4, 2024

(reflexive) $f(X) \equiv f(X) \pmod{P(X)} \Leftrightarrow P(X) \mid (f(X) - f(X))$. However, $f(X) - f(X) = 0$ and any polynomial divides 0.

(symmetric) Suppose $f(X) \equiv g(X) \pmod{P(X)} \Leftrightarrow P(X) \mid (f(X) - g(X))$. It follows $P(X) \mid (g(X) - f(X))$. Thus, $g(X) \equiv f(X) \pmod{P(X)}$

(transitive) Suppose $f(X) \equiv g(X) \pmod{P(X)}$ and $g(X) \equiv h(X) \pmod{P(X)}$. It follows $P(X) \mid (f(X) - g(X))$ and $P(X) \mid (g(X) - h(X))$. Thus, $P(X) \mid ((f(X) - g(X)) + (g(X) - h(X))) \Rightarrow P(X) \mid (f(X) - h(X)) \Leftrightarrow f(X) \equiv h(X) \pmod{P(X)}$.

2. Suppose $f_1(X) \equiv f_2(X) \pmod{P(X)}$ and $g_1(X) \equiv g_2(X) \pmod{P(X)}$. Thus, $P(X) \mid (f_1(X) - f_2(X))$ and $P(X) \mid (g_1(X) - g_2(X))$.

   $P(X) \mid ((f_1(X) - f_2(X)) + (g_1(X) - g_2(X)))$
   $\Rightarrow P(X) \mid ((f_1(X) + g_1(X)) - (f_2(X) + g_2(X)))$
   $\Leftrightarrow f_1(X) + g_1(X) \equiv f_2(X) + g_2(X) \pmod{P(X)}$.

   $P(X) \mid (g_1(X)(f_1(X) - f_2(X)) + f_2(X)(g_1(X) - g_2(X)))$
   $\Rightarrow P(X) \mid (f_1(X)g_1(X) - f_2(X)g_2(X))$
   $\Leftrightarrow f_1(X)g_1(X) \equiv f_2(X)g_2(X) \pmod{P(X)}$

3. $8X^4 - 12X^3 + 8X - 3 = (2C - 1)(4X^3 - 4X^2 - 3X + 2) + 2X^2 + X - 1$
   $4X^3 - 4X^2 - 3X + 2 = (2X - 3)(2X^2 + X - 1) + 2X - 1$
   $2X^2 + X - 1 = (X + 1)(2X - 1) + 0$
   $\gcd(8X^4 - 12X^3 + 8X - 3, 4X^3 - 4X^2 - 3X + 2) = X - \frac{1}{2}$

4.

	$y(x)$	$z(x)$
$X^3 + 2X + 2$	1	0
$X^2 + 3X + 4$	0	1
$2X + 4$	1	$4X + 3$
2	$2X + 3$	$2X^2 + X + 4$

   $1 = (X + 4)(X^3 + 2X + 2) + (X^2 + 3X + 2)(X^3 + 2X + 2)$

5. (a) If x and $p - 1$ are coprime, there exists some integer y s.t $xy \equiv 1 \pmod{p - 1}$.
   Because $g_2 \equiv g^x \pmod{p} \Rightarrow g_2^y \equiv g^{xy} \equiv g^{k(p-1)} \cdot g \equiv g \pmod{p}$ by

Fermat's Little Theorem.
Suppose $m \in \{0, 1, \ldots, p-1\}$. Because g is a primitive root, there exists some q s.t $g^q \equiv m \pmod{p}$. Let $q' \equiv qy \pmod{p}$. $g_2^{q'} \equiv g_2^{qy} \equiv g^q \equiv m \pmod{m}$. Thus, for any arbitrary $m \in \{0, 1, \ldots, p-1\}$, there exists an exponent q' s.t $g_2^{q'} \equiv m \pmod{p}$. (Surjectivity+finite domain and codomain of smae size implies a bijection) Thus, g_2 is a primitive root.

(b) Suppose x is not coprime to $p-1$. It follows there exists some proper divisor $k = \frac{p-1}{\gcd(p-1,x)} \in \mathbb{F}_{|}$ of $p-1$ s.t $xk \equiv 0 \pmod{p-1}$. Since $h^k \equiv g^{xk} \equiv 1 \pmod{p}$ then h only cycles through $k < p$ elements of $\mathbb{F}_{|}$, so h is not a primitive root.

(c) $\phi(p-1)$ because we want the number of integers less than $p-1$ that are coprime to $p-1$

6. (a) $600 = 2^3 \cdot 3 \cdot 5^2$. If $r \mid 600$, then r must share all of it's prime factors with 600. It follows $r = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3}$ where $k_1 \leq 3, k_2 \leq 1$ and $k_3 \leq 2$. Since $r < 600$, at least of of the inequalities must be strict. If $k_1 < 3 \Rightarrow r \mid 300, k_2 < 0 \Rightarrow r \mid 200$, and $k_3 < 2 \Rightarrow r \mid 120$.

   (b) Since 601 is prime, $\phi(601) = 600$. k is the smallest integer s.t $7^k \equiv 1 \pmod{601}$, so $k \mid \phi(601)$ by previous hw. Thus, by part (a), if $k < 600 \Rightarrow k \mid 120, 200$, or 300.

   (c) $7^{300} = 600 \pmod{601}, 7^{120} \equiv 423 \pmod{601}, 7^{200} \equiv 576 \pmod{601}$. If k divided $120, 200$, or 300 then at least one of our computed exponentiations would be congruent $1 \pmod{601}$.

   (d) If $k \mid 600$, but $k \nmid 120, k \nmid 200$, and $k \nmid 300$, then $k \geq 600$. Thus, $k = 600$ by definition of being the smallest integer s.t $7^k \equiv 1 \pmod{601}$. Hence, 7 must be a primitive root. If it weren't, there would be two integers q_1, q_1 where $|q_1 - q_2| < 600$ s.t $7^{q_1} \equiv 7^{q_2} \pmod{601} \Rightarrow 7^{|q_1 - q_2|} \equiv 1 \pmod{601}$ (because multiplication is well defined) which contradicts that 600 is the smallest integer s.t $7^k \equiv 1 \pmod{601}$.

7. Let $m_i = \frac{p-1}{q_i}$. If $g^{m_i} \not\equiv 1 \pmod{p}$ for all i, then g is a primitive root.

8. $65537 = 2^{16} + 1$. It follows we just need to show $3^{2^{15}} \not\equiv 1 \pmod{65537}$. Using Python $3^{2^{15}} \equiv 65536 \pmod{65537}$, so 3 is primitive root.

9. (a) $\left(3^k\right)^{32} \equiv 3^{32k} \equiv 2^{32} \equiv 1 \pmod{65537} \Rightarrow 2^{16} \mid 2^5 k \Rightarrow 2^{11} \mid k$ where $2^{11} = 2048$ Since $\left(3^k\right)^{16} \equiv 3^{16k} \equiv 2^{16} \equiv -1 \pmod{65537} \Rightarrow 2^{16} \nmid 2^4 k \Rightarrow 4096 \nmid k$ where $2^{12} = 4096$

   (b) We only need to check the odd multiples of 2048, $i = 1, 3, \ldots 31$. We obtain $3^{55296} \equiv 2 \pmod{65537}$

10. (a) X and $X+1$ are clearly irreducible because they are degree 1. $X^2 + X + 1$ is irreducible because it has no roots in $\mathbb{F}_2$. There are $2^2 = 4$

polynomials of degree 2 with coefficients in $\mathbb{F}_p$, so we need to check X^2, X^2+1 and X^2+X are all reducible. X^2+X can be reduced into polynomials X and $X+1$. X^2 can be reduced into polynomials X and X. X^2+1 can be reduced into polynomials $X+1$ and $X+1$.

(b) If X^4+X+1 is reducible, then it must be factor into polynomials of degree 2 and 2 or 3 and 1. We do division with remainder on X^4+X+1 to check if X, $X+1$, or X^2+X+1 are factors.
$X^4+X+1 = (X^3+1)X+1$
$X^4+X+1 = (X^3+X^2+X)(X+1)+1$
$X^4+X+1 = (X^2+X)(X^2+X+1)+1$
Since X^4+X+1 doesn't have any linear or quadratic factors, it must be irreducible.

(c) $X^4 \equiv X+1 \pmod{X^4+X+1} \Leftrightarrow X^4+X+1 \mid (X^4-(X+1))$.
$X^4-(X+1) \equiv X^4+X+1 \equiv 0 \pmod{X^4+X+1}$.
Since multiplication is well defined $X^8 \equiv (X^4)^2 \equiv (X+1)^2 \equiv X^2+1 \pmod{X^4+X+1}$ and $X^{16} \equiv (X^8)^2 \equiv (X^2+1)^2 \equiv X^4+1 \equiv (X+1)+1 \equiv X \pmod{X^4+X+1}$.

(d) Since X and X^4+X+1 are coprime X has an inverse $\pmod{X^4+X+1}$. It follows $X^{15} \equiv X^{-1}X^{16} \equiv X^{-1}\cdot X \equiv 1 \pmod{X^4+X+1}$

11. (a) X^2+1 doesn't have any roots in $\mathbb{F}_3$, so it must be irreducible. $0^2+1 = 1, 1^2+1 = 2, 2^2+1 = 2$.

(b) Extended Euclidean Algorithm

	$y(X)$	$z(X)$
X^2+1	1	0
$2X+1$	0	1
2	1	$X+1$

$(2X+1)(2X+2) \equiv X^2+2 \equiv 1 \pmod{X^2+1}$. $2+2X$ is the inverse of $1+2X$.